ISSN 1066-369X, Russian Mathematics, 2017, Vol. 61, No. 11, pp. 26–33. © Allerton Press, Inc., 2017.
Original Russian Text © Sh.T. Ishmukhametov, B.G. Mubarakov, K.M. Al-Anni, 2017, published in Izvestiya Vysshikh Uchebnykh Zavedenii. Matematika, 2017, No. 11, pp. 30–38.

Calculation of Bezout's Coefficients for the k-Ary Algorithm of Finding GCD

Sh. T. Ishmukhametov[1*], B. G. Mubarakov[1], and Kamal Al-Anni Maad[2***]**

[1] *Kazan Federal University*
ul. Kremlyovskaya 18, Kazan, 420008 Russia
[2] *University of Strasbourg,*
4 Rue Blaise Pascal, Strasbourg, 67081 France

Received June 24, 2016

Abstract—Bezout's equation is a representation of the greatest common divisor d of integers A and B as a linear combination $Ax + By = d$, where x and y are integers called Bezout's coefficients. The task of finding Bezout's coefficients has numerous applications in the number theory and cryptography, for example, for calculation of multiplicative inverse elements in modular arithmetic. Usually Bezout's coefficients are caclulated using the extended version of the classical Euclidian algorithm.
We elaborate a new algorithm for calculating Bezout's coefficients based on the k-ary GCD algorithm.

DOI: 10.3103/S1066369X17110044

Keywords: *Euclidean algorithm, extended Euclidean algorithm, k-ary GCD algorithm, calculation of inverse elements by module.*

INTRODUCTION

The classical Euclidean algorithm is used to calculate the greatest common divisor of given integers A and B. The algorithm uses the recurrent equality $\mathrm{GCD}(A, B) = \mathrm{GCD}(B, A \bmod B)$ several times until the second argument B of a pair (A, B) becomes equal 0, then the first argument A is the required GCD of original arguments.

The extended version of the Euclidean algorithm is used to find together with GCD d so-called Bezout's coefficients which are coefficients of a linear combination $Au + Bv = d$. The work of the extended Euclidean algorithm consists of two stages. The first stage coincides with the standard algorithm with accumulation of integers $q = [A/B]$. At the second stage the Bezout coefficients are calculates by formulas

$$u_n = 0, \;\; v_n = 1; \;\; u_i = v_{i+1}; \;\; v_i = u_{i+1} - v_{i+1} \cdot [A/B]_i, \tag{1}$$

where n is a number of the last iteration.

An example of an extended Euclidean Algorithm calculation is given in Table 1 for integers $A = 117$, $B = 41$.

The number of iterations n is 5. We assign to u_5 and v_5 values 0 and 1, respectively, and calculate other values u_i, v_i for $i < n$ by formulas (1).

The extended Euclidean algorithm can be used to find inverse elements by the given module. For example, for calculation of $a^{-1} \bmod n$ for co-prime integers a and n we need to form a table like Table 1 by setting $A = n$, $B = a$, then calculated v_1 will be equal $a^{-1} \bmod n$. In particular, from example of Table 1 we obtain $41^{-1} \equiv 20 \pmod{117}$.

*E-mail: Shamil.Ishmukhametov@kpfu.ru.
**E-mail: mubbulat@mail.ru.
***E-mail: maadk_anni@live.com.